UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with sachinmakade19@gmail.com and sachinmakde19@gmail.com that are stored at premises controlled by Google, 1600 Amphitheatre Parkway in Mountain View, California.

Case No. 19-M-008

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Scott Simons, DEA
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Jan. 10, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable David E. Jones, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Scott Simons, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, Inc. ("Google") an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer assigned to the Milwaukee District Office of the Drug Enforcement Administration (DEA) as a member of the Tactical Diversion Squad (TDS) specializing in pharmaceutical investigations. I have worked full-time as a Federal Task Force Officer for the past 5 years and a full-time law enforcement officer with the Greenfield Police Department for the past 16 years. During my tenure as a DEA Task Force Officer and a Greenfield Police Department law enforcement officer, I have been involved in the investigation of narcotics traffickers operating not only in the County of Milwaukee and the State of Wisconsin but also other states throughout the United States. I have received training in the investigation of drug trafficking and computer related crimes. I have worked with informants in the investigations of drug trafficking in the Milwaukee area as well as other jurisdictions within the State of Wisconsin

and throughout the United States. I have participated in the application for and execution of numerous search warrants. I have participated directly in numerous narcotics investigations and arrests in which controlled substances and drug paraphernalia were seized. I am familiar with methods that are commonly used by drug dealers to package and prepare controlled substances for sale in various areas.

3. The statements in this affidavit are based on my personal knowledge, information I have received from other law enforcement personnel, publicly available information, and from persons with knowledge of relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation.

4. Based on the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the information associated with the accounts identified in Attachment A, will contain fruits, evidence, and instrumentalities related to violations of Title 21, United States Code, Sections 846 and 841(a)(1) (Distribution of Controlled Substances), and Title 21, United States Code, Sections 841(h) and 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet) (the "Subject Offenses"), as further described in Attachment B.

BACKGROUND OF THE INVESTIGATION

5. In February of 2015, the Milwaukee District Office of the DEA initiated an investigation into the internet pharmacy GOLDPHARMA24 located at www.goldpharma-24.com, which advertises for sale controlled and non-controlled pharmaceuticals, including schedule II controlled substances, without requiring a prescription for such substances. During the course of the investigation of GOLDPHARMA24, case agents identified multiple Google and Yahoo

accounts used to facilitate the commission of the Subject Offenses. As described below, probable cause exists to believe the Google accounts associated with the email addresses identified in Attachment A were used to facilitate the commission of the Subject Offenses.

STATUTORY BACKGROUND

6. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 amended the Controlled Substances Act to address online pharmacies, codified at Title 21, United States Code (U.S.C.), § 829. No controlled substance that is a prescription drug as determined by the Federal Food, Drug and Cosmetic Act may be delivered, distributed, or dispensed by means of the Internet without a valid prescription, as required by Title 21, Code of Federal Regulations (C.F.R.) § 1306.09(a). *See* Title 21, U.S.C. § 829(e), § 841(a)(1) (Distribution of Controlled Substances); 21 U.S.C. § 841(h), § 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet). According to Title 21 U.S.C. § 829, the term "valid prescription" means a prescription that is issued for a legitimate medical purpose in the usual course of professional practice by a practitioner who has conducted at least 1 in-person medical evaluation of the patient or a covering practitioner. The term "in-person medical evaluation" means a medical evaluation that is conducted with the patient in the physical presence of the practitioner, without regard to whether portions of the evaluation are conducted by other health professionals. The term "covering practitioner" means, with respect to the patient, a practitioner who conducts a medical evaluation (other than an in-person medical evaluation) at the request of a practitioner who has conducted at least 1 in-person medical evaluation of the patient or an evaluation of the patient through the

practice of telemedicine within the previous 24 months and is temporarily unavailable to conduct the evaluation of the patient.

7. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 also added new provisions to prevent the illegal distribution of controlled substances by means of the Internet, including registration requirements of online pharmacies, Internet pharmacy website disclosure information requirements, and prescription reporting requirements for online pharmacies. According to C.F.R. § 1301.11(b):

> As provided in sections 303(f) and 401(h) of the Act (21 U.S.C. 823(f) and 841(h)), it is unlawful for any person who falls within the definition of "online pharmacy" (as set forth in section 102(52) of the Act (21 U.S.C. 802(52)) and § 1300.04(h) of this chapter) to deliver, distribute, or dispense a controlled substance by means of the Internet if such person is not validly registered with a modification of such registration authorizing such activity (unless such person is exempt from such modified registration requirement under the Act or this chapter).

8. According to DEA records, Goldpharma24 (a primary target of this investigation) is not a registered online pharmacy.

PROBABLE CAUSE

9. Throughout the course of this investigation, case agents from the DEA Milwaukee District Office (MDO) applied for and obtained federal search warrants for multiple email accounts for individuals affiliated with the distribution of illegal pharmaceutical products and illegal distribution of controlled substances. A review of these emails revealed at least one source of supply was able to ship controlled substances from both India and Singapore. Case agents also conducted multiple online controlled buys from the online pharmacy GOLDPHARMA24, which is owned and operated by multiple identified people located in Argentina. GOLDPHARMA24 is then sourced by various sources of supply located throughout the world, but mostly in India, Eastern Europe, and United Kingdom. It was learned that GOLDPHARMA24 began seeking new

sources of supply in the beginning of 2018, after one of its primary sources of supply located in Romania was arrested by Romanian and U.S. Authorities in January 2018.

10. On August 12, 2018, case agents conducted an undercover purchase from the GOLDPHARMA24 internet pharmacy at website www.goldpharmanew.com. Case agents purchased 200 tablets of Tapentadol 100mg (which is a schedule II controlled substance). In connection with the purchase, case agents were instructed, via email, to wire money by Money Gram to ANDREY MUSOKHRANOV in Russia. Case agents received a shipment from Singapore of 220 tablets of Tapentadol 100mg. These tablets were packaged in blister packs consistent with how they would come packaged from a manufacturer. These blister packs identified the tablets as Tapentadol 100mg and were labeled as manufactured in India by Indian company HAB Pharmaceuticals and Research Limited.

11. Case agents examined the shipping material the Tapentadol was shipped in. The sender was listed on the shipping material as:

Azesto Impex PTE LTD
Changi Airfreight Centre
PO Box 1240
918119
Singapore 068892

12. DEA New Delhi Country Office (India) Diversion Investigator Ann Chi reviewed U.S. Customs and Border Protection records documenting seized packages shipped by Azesto Impex PTE LTD, with an address in India, destined for the United States and originating from India. Since 2015 to present, there have been approximately 208 of these seizures weighing a total of 161.3 pounds. These packages contained tapentadol (schedule II controlled substance), carisoprodol (schedule IV controlled substance), tramadol (schedule IV controlled substance),

etizolam (not approved by the DEA or FDA in the U.S.), modafinil (schedule IV controlled substance), and tadalafil (prescription drug).

13. Case agents received records from DEA Kuala Lumpur (Malaysia) SA Laurence Madariaga who oversees enforcement in Singapore. SA Madariaga received records pertaining to the shipper's P.O. Box in Singapore from Singaporean Law Enforcement. These records identify the P.O. Box account holder as follows:

> Business name: Azesto Impex Pte Ltd
> Address: 80 Robinson Road #11-01 Bank of East Asia Bldg, Singapore 068892
> Phone number: 91-9371020344 (Indian phone number)
> Applicant's name: SACHIN PANDHURANG MAKDE
> Email: **sachinmakde19@gmail.com**
> Start date: March 27, 2018

14. Case agents reviewed Indian open source database Zaubacorp, which identifies businesses registered in India. Azesto Impex Private Limited is registered in India. The registration lists SACHIN MAKADE PANDURANG as one of the business's directors using email address **sachinmakade19@gmail.com**.

15. An open source search of **sachinmakade19@gmail.com** shows it is associated with B.S. Exports and B.S. Medicine & Foods Private Limited which are both located in India. B.S. Medicine & Foods and Azesto Impex Private Limited both have the same listed address in India.

16. Case agents reviewed open source records of the Data Universal Numbering System (DUNS). The DUNS is a worldwide universal identifier issued to an entity based on a request from that entity to receive a DUNS number. The information provided to the DUNS system is provided specifically by that entity requesting the DUNS number. Case agents found Azesto Impex Private Limited has a DUNS number 87-685-1362 with an address in India. The DUNS record indicates the alleged type of business is a candy, nut, and confectionary store with

annual sales of $2,642,856 USD. A second DUNS number 65-948-5108 was located for Azesto Impex PTE, LTD. This DUNS listing shows this business is registered with an address of 60 Robinson Road, #11-01 BEA Building, Singapore 068892. (This address is almost identical to the address listed for the drug shipper's P.O. Box in Singapore.) This DUNS record indicates the alleged type of business is a catalog and mail-order house with annual sales of $396,267 USD. Based on these two DUNS numbers, case agents believe Azesto Impex registered in both India and Singapore because the same entity is doing business in both countries.

17. Case agents received records from Google related to email addresses **sachinmakade19@gmail.com** and **sachinmakde19@gmail.com** in response to a DEA Administrative Subpoena. Case agents reviewed the following records for these two email addresses:

1. Email: **sachinmakde19@gmail.com**
   Name: SACHIN MAKDE
   Recovery Email: shrigajanan@ymail.com
   Account creation: created on 02-15-2013 from Indian IP address 203.192.225.77
   Phone: +91-8806607635 (Indian)

2. Email: **sachinmakade19@gmail.com**
   Name: SACHIN MAKADE
   Recovery Email: sachin.makade82@gmail.com
   Account creation: created on 09-23-2013
   Phone: +91-9766284028 (Indian)
   IP login: numerous recent Indian IP addresses

18. Google records acquired by DEA Administrative subpoena also showed email address **sachinmakade19@gmail.com** was used to create a YouTube account on October 29th, 2013 from an Indian IP address. The name provided for this YouTube account is also SACHIN MAKADE. Case agents viewed this publicly accessible YouTube page which had one posted video of what appeared to be Indian music. The photograph used for this YouTube account's

profile depicted various types of prescription pills and what appeared to be "BS Export". (As previously mentioned by affiant, B.S. Exports and B.S. Medicine & Foods Private Limited is associated with **sachinmakade19@gmail.com** per an open source search.)

19. Based on my training and experience and the provided facts, I believe SACHIN MAKADE, or someone utilizing this alias, is involved in a drug trafficking organization (DTO) that ships controlled pharmaceuticals from India to the United States. I also know that shipments of controlled substances are frequently seized by Indian and U.S. authorities when shipped directly from India to the United States. As a result, Singapore is a common intermediary country for drug shipments to be routed through from India prior to being shipped to the United States.

20. In addition, I also believe based on my training and experience and the provided facts, that information related to the email addresses **sachinmakade19@gmail.com** and **sachinmakde19@gmail.com** will include evidence about the DTO. More specifically, the email address **sachinmakde19@gmail.com** is associated with the Singaporean P.O. Box for the drug shipper. I know from my training and experience that email records, to include the email content, will often times provide details that enable law enforcement to identify the user of the email and pinpoint his or her location. In this case, the identification of the user of the email accounts will assist case agents in identifying the true identity and location of the person(s) having control over the Singaporean P.O. Box, from which drugs are being illegally shipped into the United States.

21. I also know that persons involved with owning and/or operating internet pharmacies and providing the drugs for such internet pharmacies most often communicate by email. These communications include but are not limited to drug orders, drug shipping information, and payments for said drugs. In this investigation specifically, I have had the opportunity to review email account records, to include email content, belonging to multiple members of this DTO which

were obtained pursuant to federal search warrants. Based on the review of these records, from speaking to customers, by conducting undercover controlled buys, and speaking with cooperating co-conspirators, I know that email is the primary form of communication for this DTO. Most commonly, customers place their orders by email or by internet pharmacy website. Internet pharmacy representatives communicate with the customers by email regarding payment and drug order. The internet pharmacy representative then emails the orders to the internet pharmacy employee responsible for forwarding the orders to the source of supply. After the source of supply ships the drugs to the customer(s), an email is commonly sent by the source of supply to the internet pharmacy representative documenting that the order was shipped and the tracking number. Upon request by the customer, the internet pharmacy representative will email the shipping tracking number to the customer. In addition, the internet pharmacy employees will also communicate, via email, with the source of supply about payment for the controlled substances.

22. One source of the internet pharmacy's supply, as revealed by undercover controlled buys, is Azesto Impex Private Limited. As described above, that business is believed to be utilizing email addresses **sachinmakade19@gmail.com** and **sachinmakde19@gmail.com.** As a result, there is probable cause to believe that email addresses **sachinmakade19@gmail.com** and **sachinmakde19@gmail.com** are being used to communicate with other DTO members to further the work of the DTO, in the manner described above.

23. For all of the foregoing reasons, case agents are requesting a search warrant for emails containing the information set forth in Attachment A for the following: **sachinmakade19@gmail.com** and **sachinmakde19@gmail.com** for the time period of January 1, 2015 to the present. This is the time period that U.S. Customs and Border Protection records

show numerous drug shipments being shipped by Azesto Impex Pte. Ltd. to the United States have been seized.

24. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period.

BACKGROUND CONCERNING GOOGLE

25. In my training and experience, I have learned that Google provides a variety of online services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain a free email account at the domain name gmail.com like the Subject Account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

27. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

28. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

29. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically

retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. In addition to email, Google offers its users a number of other online services. A list of those services and their feature is available at the following URL: https://support.google.com/.

31. One of the services Google offers is Google Drive. Google Drive is a file storage and file sharing application that allows its users to share access to the content of files by sending a URL to others. According to information available from Google, Google stores the content of those files on their servers. In my training and experience, information stored on Google Drive may constitute evidence of the crimes under investigation because the information may include records of illicit transactions, payment ledgers, and similar documents.

32. In my training and experience, and publicly available information from Google, I know that Google uses cookies and similar technology to collect information about its users, including to identify a user's device and browser version. Google also states that it uses "technologies" to determine a user's actual location. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users and their locations.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 2713 by using the

warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

34. Pursuant to 18 U.S.C. § 2713, this application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

CONCLUSION

35. Based on the information described above, I request that the Court issue the proposed search warrant for the Subject Accounts. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

36. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following email addresses and for the following time periods, that are stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain View, California.

1. **sachinmakade19@gmail.com** (from January 1, 2015 to present)
2. **sachinmakde19@gmail.com** (from January 1, 2015 to present)

ATTACHMENT B

Particular Things to be Disclosed and Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each of the accounts or identifiers listed in Attachment A:

a. All customer information (e.g. name, age, email address, physical address, payment information, telephone numbers) associated with the account;

b. All records and information regarding the creation of the account and access to the account, including records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, and log-in IP addresses associated with session times and dates.

c. The types of services utilized;

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

e. All records, files, and other information stored/saved in the accounts, including information, files, and data saved to Google Drive;

f. A complete file activity log for any associated Google Drive account;

g. All records and information and analytics collected by the Provider through the use of cookies or similar technology including the type of browser and device used by the account holder to access the account, the web page visited before coming to Google sites, and other identifiers associated with the devices used by the account holder;

h. All records and information that identifies a user's actual location;

i. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken;

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of the warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities related to violations of Title 21, United States Code, Sections 846 and 841(a)(1) (Distribution of Controlled Substances), and Title 21, United States Code, Sections 841(h) and 843(c)(2)(A) (Offenses involving distribution of Controlled Substances by means of the Internet), since January of 2015, including but not limited to, information pertaining to the following matters:

a. The sale and distribution of controlled substances;

b. The exchange or laundering of funds related to the sale and distribution of controlled substances;

c. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

d. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

e. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s)

f. Other accounts used by the persons using the account;

g. The devices used to access the account;

h. The identity of the person(s) who communicated with the account about matters relating to the sale and distribution of controlled substances, including records that help reveal their whereabouts;

i. The identity of persons sharing Google Drive account URLs associated with the account and related to the sale and distribution of controlled substances;

j. The identity of persons saving, storing, editing, and accessing files and records on Google Drive accounts associated with the account and related to the sale and distribution of controlled substances;

k. Financial information, credit card numbers, social security numbers, and other personal identifiable information stored on/in Google Drive account; and

l. Communications and files that contain IP addresses and username and passwords to those IP addresses.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____ [Provider], and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of _____ [Provider]. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of _____, and they were made by _____ [Provider] as a regular practice; and

b. such records were generated by _____ [Provider] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of _____ [Provider] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by _____ [Provider], and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature